REMARKS

Claims 1-13 are pending in the instant application (hereinafter, the "'320 Application"). It is believed that the following remarks address and resolve each rejection presented in the Office Action mailed 08 October 2008.

Response to Amendment

Applicants thank the Examiner for indicating withdrawal of the objections and rejections laid out in the office action of 09 July 2008.

Claim Rejections – 35 U.S.C. § 102 - Vallee

Before delving into the specific claim rejections, Applicants note that the Examiner has used the same 19-paragraph section of U.S. Patent Application Publication No. US 2004/0177252 (hereinafter, "Vallee") in rejecting 5 steps of claim 5, the additional features of claim 6, and the 10 steps of claim 7. However, the Examiner has not identified which specific features of Vallee supposedly anticipate which steps/features of Applicants' claims. This leaves Applicants having to guess at what the Examiner is thinking, which does not facilitate the development of clear issues between Applicants and the Examiner. See MPEP §706.07. Accordingly, if the Examiner upholds any rejection after review of the following arguments, we respectfully request detailed reasons for rejection, specifically pointing out which features of Vallee are believed to anticipate which features of Applicants' claims. However, it is believed that the arguments below show that regardless of what comparisons the Examiner means to make, Vallee does not anticipate claims 5-7.

Turning now to the rejections set forth, claims 5-7 stand rejected under 35 U.S.C. §102(e) as being anticipated by Vallee. Applicants respectfully disagree. In order to anticipate claims 5-7, Vallee must teach every element of each claim and "the ***identical invention*** must be shown in as complete detail as contained in the ... claim." *MPEP 2131*, citing *Verdegaal Bros. V. Union Oil Co. of California*, 814 F.2d 628, 2 USPQ2d 1051 (Fed. Cir. 1987) and *Richardson v. Suzuki Motor Co.*, 868 F2.d 1226, 9 USPQ2d 1913 (Fed. Cir. 1989), emphasis added.

Independent Claim 5: Thus, in order to anticipate claim 5, Vallee must teach a method of protecting a host from unauthorized client access over a network, including the following steps:

(a) installing a prover agent application on the client;

(b) installing a verifier agent application on the host;

(c) creating a trusted source application to generate and publish encrypted values of a secret and product of first and second large prime numbers;

(d) reading the encrypted values for the secret and product, by the prover and verifier from the trusted source;

(e) decrypting the secret, by the prover and verifier;

(f) decrypting the product, by the prover and verifier; and

(g) performing a plurality of verification dialog between the prover and verifier, wherein the prover demonstrates knowledge of the secret and product without exposing the values of the secret and product, and wherein the client is denied access to a secure area of the host when the prover fails to demonstrate knowledge of the secret and product and granted access to the secure area when the client succeeds in demonstrating knowledge of the secret and product.

However, Vallee does not teach each of the above steps, nor does Vallee show the steps in as complete detail as shown in the claim.

First, claim 5 recites generation and publication (by a trusted source application) of encrypted values of a secret and a product of first and second large prime numbers. See step **(c)**, above. The cited Vallee section (paragraphs [0090]-[0108]) does not anticipate this feature, nor does Vallee elsewhere teach or suggest this generation and publication. Vallee recites a confidence authority, whose role "is to compute the secret keys of users of the method," Vallee paragraph [0093]. It appears that the confidence authority also has knowledge of a public key (*Kv*). See paragraph [0094]. However, there is no teaching of generating and publishing encrypted values of a product of first and second large prime numbers. For example, the cited section does not teach multiplying two large prime numbers, and then encrypting their product. Regarding prime or non-prime numbers, Vallee recites only that the public key *Kv* is an integer less

than a large non-prime integer *n* (known only to the confidence authority). See Vallee paragraph [0093]. This is different from generating/publishing encrypted values garnered from a product of first and second large prime numbers. Because Vallee does not teach generation or publication of encrypted values of a product of first and second large prime numbers, Vallee also cannot and does not recite decryption of such a product, as in step **(f)**.

Next, claim 5 specifically recites that a client is denied or granted access *to a secure area of a host* based on the prover's ability to demonstrate knowledge of a secret and product (see step **(g)**). Vallee does not recite or even suggest granting or denying access to a secure area of a host. Vallee only discusses providing or denying services (e.g., telecommunication equipment) or electronic funds transfer, based upon the results of an authentication attempt. See Vallee paragraphs [0176]-[0186]. These are different from granting or denying access to a secure area of a host.

As shown above, Vallee does not teach (or even suggest) all features of claim 5; accordingly, Vallee cannot and does not anticipate the claim.

Dependent Claims 6 and 7: These claims depend from claim 5, and thus benefit from the above argument. However, claims 6 and 7 also include other features that are patentably distinct from Vallee. For example, **claim 6** recites that decrypting uses previous values of the secret and product as operators in a modulus inverse operation. The Examiner cites Vallee paragraphs [0090]-[0108] in an attempt to establish anticipation of this feature. However, this section is silent as to previous values of secrets and products. And Vallee does not elsewhere teach that previous values of the secret and product are used as operators during decryption.

Among other steps, **claim 7** recites:

(a) calculating x by the first agent, r (a random number generated by the first agent) being raised to power of t modulus n;

(b) calculating b by the second agent, b being further defined as a member of set of integers from zero through t-1; and

(c) calculating y by the first agent, y being a product of r*s raised to power of b.

The Examiner has not specified which operators of Vallee paragraphs [0090]-[0108] are likened to Applicant's operators (e.g., x, r, t, b, y). Therefore, it is exceedingly difficult to formulate a proper response, since Applicants are again left having to guess at how the Examiner interprets Vallee. Applicants guess that the Examiner is drawing comparisons between similarly identified operands in the '320 Application and Vallee (i.e., comparing Applicants' x, r, s and n to Vallee's x, r, s and n). Applicants also believe that the Examiner is likening b to Vallee's "random bit e" and y to Vallee's "response C". If this is incorrect, Applicants request that the Examiner explicitly identify each teaching of Vallee that is compared to each feature of claim 7, so that an appropriate response can be made.

Note that claim 7 recites r being raised to power of t modulus n. Vallee shows r^2modn. Thus, Applicants believe that the Examiner means to compare t (of claim 7) to 2 (in Vallee). If that is correct, then in order to anticipate step **(b)**, above, Vallee would have to define b as being a member of a set of integers from zero through 2-1. However, Vallee does not define b in this way. Accordingly, Vallee does not anticipate step **(b)**.

Step **(c)**, above, recites that y is a product of r*s raised to power of b. Accordingly, if Applicants have correctly identified the Examiner's comparisons between the '320 Application and Vallee (e.g., comparing Applicants' y and b to Vallee's "response C" and "random bit e"), in order to anticipate step **(c)**, Vallee must teach that response C is a product of r*s raised to power of random bit e. However, Vallee does not teach or suggest such an equation. See, for example, Vallee paragraph [0100]. Vallee does not use random bit e as an exponent.

Thus, Vallee fails to teach or suggest at least two features of claim 7. If the Examiner maintains the current rejection, we again respectfully request that the Examiner point out which specific items in Vallee are said to anticipate which specific features of Applicants' claims.

As shown above, Vallee does not teach every feature of claims 5-7. Applicants therefore respectfully request withdrawal of the instant §102 rejection, and allowance of claims 5-7.

Claim Rejections – 35 U.S.C. § 103 – Bartram in view of "Admission"

Claims 1, 8 and 13 stand rejected under 35 U.S.C. Section 103(a) as being unpatentable over U.S. Patent Publication No. 2004/0054885 (hereinafter, "Bartram"), in view of a purported "Admission" found at pages 1-3 of the '320 Application. Applicants respectfully traverse the rejection.

Claims 1, 8 and 13 require that a first computer has both a first authentication agent and a first prover agent. The Examiner cites only the authentication software of Bartram as representing these two claimed elements; differentiation requires that each of these elements be distinctly identified within the cited art. Bartram fails to disclose both an authentication agent and a prover agent.

The Examiner admits that Bartram does not disclose zero-knowledge authentication/identification protocol. However, the Examiner states that "Applicant admits that the use of zero knowledge protocols was conventional and well known at the time the invention was made. Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to use zero knowledge authentication protocols with the invention of Bartram since it would extend authentication capabilities to other devices and other products." Office Action, page 5.

Applicants respectfully disagree. First, it must be noted that pages 1-2 include both the Background section, which, per MPEP 608.01(c), "describ[es] to the extent practical the state of the prior art or other information disclosed known to the applicant "), and pages 2-3 feature the "Summary of Invention" (which "should be directed to the specific invention being claimed", MPEP 608.01(d). Applicants believe that it is improper to use the "Summary of Invention" section (in other words, the claimed invention), as prior art against the pending claims. Accordingly, only the disclosure in the "Background" section on pages 2-3 of the '320 Application is addressed herein below.

The "Background" section of the specification identifies zero knowledge identification as a known protocol for providing authentication without transmission of a secret password. However, the Background section does not present or suggest the use of zero knowledge protocol in any network authentication and promotion method (or where

a requesting computer operates with an authentication agent on the computer network, as worded in claim 8).

The Examiner has essentially taken a statement that zero knowledge protocol exists, and used that statement to justify an unsupported personal opinion as to why zero knowledge protocol could be combined with Bartram. Respectfully, this is improper. As codified in Section 2143.01 of the MPEP, *prima facie* obviousness cannot be established by merely picking and choosing unrelated features from various references. Instead, the Examiner has the additional required burden to additionally indicate in the written record where the prior art itself (absent, as in the present case, any evidence in the record of some well-known principle in the art) affirmatively teaches or suggests the motivation to combine the references as proposed. Applicants note that neither the "Background" nor Bartram teach that Bartram's peer-to-peer authentication should or could be coupled with zero knowledge protocol.

More specifically, for authentication, Bartram utilizes certificates and digital signatures. See at least Bartram paragraphs [0034-0035]. As disclosed in paragraph [0010] of Bartram, "each peer obtains a copy of the other's certificate" and "each peer has its own self-signed certificate and private key." These certificates and digital signatures utilize a concept of public and private key pairs; a concept that is very different from the zero knowledge authentication protocol wherein no certificate is exchanged. Bartram thus teaches away from the use of a zero knowledge protocol that requires no certificate or digital signature.

Because the Examiner has not pointed to a prior art teaching supporting the proposed motivation to combine Applicants' own specification with Bartram, the stated rationale to justify the combination is essentially based upon the Examiner's own personal opinion. The Federal Circuit, though, has expressly held that mere conclusory statements from the Examiner, without any actual evidence cited on the record in support thereof, cannot satisfy the Examiner's burden to establish the obviousness of combining the references. See *In re Lee,* 277 F.3d 1338 (Fed. Cir. 2002). See also *In re KSR International Co.,* quoted above. Applicants submit that the Examiner must provide objective evidence that it would have been obvious, at the time the invention was made,

to combine zero knowledge authentication with Bartram's peer-to-peer system; otherwise, the rejection must be withdrawn.

Without such required evidence on the record – evidence capable of objective review and rebuttal – the rejection presents nothing more than a case of impermissible hindsight. The rejection *presumes* the obviousness of combining Applicants' Specification with Bartram, based on the Examiner's own opinion. By definition, the Examiner's personal opinion can never satisfy the definition of "documentary evidence, capable of objective review and rebuttal." The Examiner, for example, has not submitted anywhere in the record how he arrived at his conclusory opinion, where he received the knowledge that forms the basis of that opinion, and the actual dates such knowledge was obtained by him. The present case therefore presents the exact situation expressly rejected by the Federal Circuit in *Lee*. The rejection of claims 1, 8 and 13 should be withdrawn for at least this reason.

Claim Rejections – 35 U.S.C. § 103 – Bartram in view of "Admission" and Vallee

Claims 2, 4 and 9-12 stand rejected under 35 U.S.C. Section 103(a) as being unpatentable over Bartram and the purported Admission described above, and further in view of Vallee. Applicants again respectfully traverse the rejection.

Claims 2 and 4 depend from claim 1. As noted above, the rejection of claim 1 is based upon an unsupported conclusory statement by the Examiner, and therefore cannot stand. Adding Vallee to the combination used to reject claim 1 does not solidify the rejection, since Vallee also fails to teach or suggest use of zero knowledge protocol in peer-to-peer authentication. Thus, the Bartram/purported Admission/Vallee combination also cannot and does not establish *prima facie* obviousness over claim 1.

Courts have ruled that if an independent claim is nonobvious under 35 U.S.C. 103, then any claim depending therefrom is nonobvious. *In re Fine*, 837 F.2d 1071.5 USPQ2d 1596 (Fed. Cir. 1988). Since claims 2 and 4 depend from claim 1, the instant rejection fails for at least this reason.

Furthermore, **regarding claim 2**, the Examiner relies fully upon Vallee for "generating and distributing a new secret to first and second authentication agents." However, the cited passage (paragraphs [0090]-[0108]) discusses only <u>one</u> authenticator entity B. The other disclosed entity is an entity to be authenticated (A). There are no

first and second authentication agents. Furthermore, the cited section of Vallee does not discuss generating a new secret. It is important to note that Vallee teaches the computation of secret key by a confidence authority. After the key is computed, entities A and B undergo multiple iterations of five exchange/computation steps (see steps 1-5 at Vallee paragraphs [0096]-[0100], see also paragraphs [0094] and [00101]. It appears that the same secret key is used in each of these iterations, since there is no teaching of generating and distributing a new secret. Since claim 2 recites generation and distribution of a new secret, it contains features not taught or suggested by the Bartram/purported Admission/Vallee combination. Accordingly, *prima facie* obviousness is not established.

Turning now to **claim 4**, the Examiner admits that Bartram and the purported Admission do not disclose the steps of claim 4. Applicants contend that, contrary to the Examiner's assertion, neither does Vallee teach these steps. For example, as noted above, Vallee does not specify *calculating a product of first and second large prime numbers*. See arguments in answer to the §102 rejections, above. Neither does Vallee generate a secret *to have a value relatively prime to the product*. For at least these reasons, the instant rejection fails.

Claims 9-12 depend from claim 8. As noted above, the rejection of claim 8 in view of Bartram and the purported Admission is based upon a conclusory personal opinion, and therefore cannot stand. Courts have ruled that if an independent claim is nonobvious under 35 U.S.C. 103, then any claim depending therefrom is nonobvious. *In re Fine*, 837 F.2d 1071.5 USPQ2d 1596 (Fed. Cir. 1988). Thus, claims 9-12 are also nonobvious, for at least this reason. However, these claims include additional features not taught or suggested by the cited art, including the following:

In rejecting **claim 9**, the Examiner admits that Bartram and the purported Admission do not teach generating a new secret. As noted above in the arguments in support of claim 2, neither does Vallee teach this feature. Accordingly, the rejection fails to establish *prima facie* obviousness.

Claim 10 recites that the requesting computer comprises a cell phone. The Examiner states that the combination of Bartram and the purported Admission teach this feature, citing paragraphs 2-3 (of which reference is not stated). Paragraph [0002] of

Bartram states "With the popularity of portable computing devices (i.e., PDA's cell phones, etc.) increasing, there comes a greater need and ability to share information between devices..." The Examiner appears to argue that a zero-knowledge authentication system (including a cell phone having a prover agent) would have been obvious simply because (a) the '320 Specification recognizes that zero-knowledge protocol exists, and (b) Bartram mentions a cell phone. However, as the Examiner admits, Bartram does not teach or suggest zero knowledge authentication. Accordingly, the motivation to combine a cell phone with a zero-knowledge authentication system does not come from Bartram. Likewise, the '320 Background section recognizes that zero-knowledge protocol exists, but does not mention its use with a cell phone. Thus, the motivation to combine zero-knowledge authentication with a cell phone as a requesting computer also does not come from the '320 Application. And the Examiner has not provided any rationale or well known principle to support the purported combination.

Again, *prima facie* obviousness cannot be established by merely picking and choosing unrelated features from various references. Instead, the Examiner has the additional required burden to additionally indicate in the written record where the prior art itself (absent, as in the present case, any evidence in the record of some well-known principle in the art) affirmatively teaches or suggests the motivation to combine the references as proposed. See Section 2143.01 of the MPEP. Since the art itself does not teach or suggest the motivation to combine a cell phone (as a requesting computer having a prover agent) in a system of non-centralized zero-knowledge authentication, in order for the instant rejection to stand, the Examiner must provide evidence (and not a personal opinion) that such a combination would have been obvious. Otherwise, *prima facie* obviousness is not established.

Claim 12 recites that authentication agents and prover agents are installed on each of the computers through common software. The Examiner appears to rely upon Bartram paragraphs 25-34 for this feature; however, this passage does not discuss authentication or prover agents. It discusses collaborative application software (i.e., software 104, FIG. 1), but authentication and prover agents are not mentioned. Furthermore, this section of Bartram discusses the exchange of certificates between computers. This is different from engaging in zero-knowledge protocol, as in base claim

8. As noted with respect to claims 1, 8 and 13, above, the acknowledgement that zero-knowledge protocol exists (in the '320 Application "Background" section) does not itself establish obviousness of a system where a requesting computer operates with an authentication agent on the network, once it is itself authenticated to the network via zero-knowledge protocol. The cited art itself does not teach or suggest the motivation to make the proposed combination, and the Examiner has not provided any documentary evidence for why such a combination would have been obvious. Accordingly, the instant rejection is deficient and should be withdrawn.

CONCLUSION

It is believed that the above remarks address and overcome each rejection presented in the office action of 08 October 2008. Applicants thus respectfully solicit a Notice of Allowance for all pending claims.

Should any of the instant rejections be reiterated, Applicants again respectfully request that the Examiner specifically point out which items in the prior art are believed to anticipate which features of the pending claims. Per MPEP §706.07, "The examiner should never lose sight of the fact that in every case the applicant is entitled to a full and fair hearing, and that a clear issue between applicant and examiner should be developed, if possible, before appeal." Using a blanket section of a reference to reject multiple specific claim features forces Applicants to guess at what comparisons the Examiner is attempting to draw, and simply does not allow for the development of clear issues.

A Petiton for Two Month's Extension of Time is filed herewith, along with authorization to charge the required $245 petition fee to Deposit Account No. 12-0600. This extends the period of reply up to, and including, 08 March 2009. No other fees are believed due; however, if any additional fee is deemed necessary in connection with this paper, please charge the aforementioned Deposit Account. Should any issues remain outstanding, the Examiner is encouraged to telephone the undersigned.

Respectfully submitted,
LATHROP & GAGE LLP

Date: 10 Feb. 2009

By: Heather Perrin

Heather Perrin, Reg. No. 52,884
4845 Pearl East Circle, Suite 201
Boulder, Colorado 80301
Tel No: (720) 931-3033
Fax No: (720) 931-3001